Dr Artur Romaszewski
Uniwersytet Jagielloński - Collegium Medicum
Wydział Nauk o Zdrowiu
Zakład Medycznych Systemów Informacyjnych

Dr hab. med. Wojciech Trąbka
Uniwersytet Jagielloński - Collegium Medicum
Wydział Nauk o Zdrowiu
Zakład Medycznych Systemów Informacyjnych

Rola i zadania administratora danych oraz podmiotu przetwarzającego w podmiotach leczniczych w świetle ustawy o ochronie danych i Rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych

We wszystkich podmiotach świadczących usługi zdrowotne trwają prace nad przygotowaniem się do wprowadzenia w życie elektronicznej dokumentacji medycznej i co jest z tym związane wdrożeniem dedykowanych do tego celu aplikacji komputerowych. Jest to znakomita okazja do tego, żeby przejrzeć funkcjonujące dokumenty związane z przetwarzaniem danych osobowych, których wymaga prawo. Od początku 2015 r. weszły w życie nowe przepisy dotyczące ochrony danych osobowych, a prawdopodobnie od 2016 r. na obszarze Unii Europejskiej zostanie wprowadzone rozporządzenie UE regulujące ochronę danych osobowych - projekt Komisji Europejskiej i Parlamentu Europejskiego[1], które zastąpi Dyrektywę UE 95/46/WE o ochronie danych osobowych.[2]

Nowe przepisy zapowiadają wprowadzenie szeregu zmian w organizacji podmiotów leczniczych. Obecnie po wejściu w życie zmian w ustawie o ochronie danych osobowych[3] część z nich jest fakultatywna i pozostawiono kierownikom podmiotów dobrowolność ich wdrożenia. Sytuacja ulegnie zmianie po wejściu w życie przepisów UE. Wówczas przepisy

[1] ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (ogólne rozporządzenie o ochronie danych) http://giodo.gov.pl/560/id_art/4503/j/pl/
[2] http://www.giodo.gov.pl/568/id_art/603/j/pl/
[3] Ustawa z dnia 7 listopada 2014 r. o ułatwieniu wykonywania działalności gospodarczej Dz. U. 2014 poz. 1662

dotyczące między innymi powołania w podmiocie leczniczym Administratora Bezpieczeństwa Informacji spełniającego określone prawem kryteria staną się obligatoryjne.

Uznano, że prawo dotyczące ochrony danych niedostatecznie chroni dane osobowe. Wprawdzie w Polsce obecnie obowiązujące przepisy ustawy o ochronie danych osobowych przewidują szereg sankcji karnych za brak respektowania obowiązujących norm prawnych, jednak przepisy rozporządzenia UE ustalają dotkliwe konsekwencje finansowe za brak wdrożenia w życie przepisów rozporządzenia UE. Chodzi przede wszystkim o zobowiązania podmiotów do stosowania odpowiednich działań wymaganych przy przetwarzaniu danych osobowych, także tych które dotyczą danych o stanie zdrowia pacjenta, a więc danych wrażliwych. Jednym z założeń przeprowadzanej reformy jest stosowanie „skutecznych, proporcjonalnych i odstraszających" sankcji administracyjnych wobec każdego, kto nie będzie spełniał obowiązków, jakie przewiduje rozporządzenie. Organ nadzoru (niezależny i bezstronny) będzie uprawniony do wymierzenia co najmniej jednej z następujących sankcji: ostrzeżenia na piśmie, w przypadku wykrycia pierwszej i niezamierzonej niezgodności; regularnej okresowej kontroli; grzywny do 100 000 000 Euro lub 5% rocznego przychodu[4] w przypadku przedsiębiorcy, w zależności od tego, która kwota będzie wyższa[5].

W polskim prawie istotne zmiany w ustawie o ochronie danych osobowych wprowadziła ustawa z 7 listopada 2014 roku o ułatwieniu wykonywania działalności gospodarczej.[6] Zmiany obowiązują od 1 stycznia 2015 r., a dotyczą przede wszystkim funkcjonowania w podmiotach Administratora Bezpieczeństwa Informacji oraz problemu przekazywania danych poza granicę Europejskiego Obszaru Gospodarczego.

W rozporządzeniu UE zdefiniowano pojęcie administratora, który podobnie jak w obowiązującej ustawie o ochronie danych osobowych jest zarówno osobą fizyczną lub prawną, organem publicznym, jednostką organizacyjną lub inny podmiotem, który

4 Poprawka 188 art. 79 ust. 2a rozporządzenia 24 Rezolucja ustawodawcza Parlamentu Europejskiego z dnia 12 marca 2014 r. w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (ogólne rozporządzenie o ochronie danych) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)

5 BLOG PROFESJONALNIE O OCHRONIE DANYCH OSOBOWYCH - J Bardadyn - Kiedy (ostatecznie!) i jak UE zreformuje prawo ochrony danych osobowych? http://blog-daneosobowe.pl/ue-ostatecznie-zreformuje-prawo-ochronie-danych-osobowych-beda-kluczowe-zalozenia/

6 Dz. U. 2014 poz. 1662

samodzielnie lub wspólnie z innymi organami (współadministrator) ustala cele, warunki i sposoby przetwarzania danych osobowych[7].

W artykule zostaną omówione najważniejsze regulacje prawne i projekty regulacji UE dotyczące funkcjonowania administratora danych jako podmiotu odpowiadającego w podmiotach leczniczych za cele i środki przetwarzanych tam danych osobowych.

Specyfika danych medycznych oraz systemu informacyjnego opieki zdrowotnej

Analizując problematykę ochrony danych w systemie opieki zdrowotnej należy podkreślić zarówno specyficzny charakter danych medycznych – dane osobowe i dodatkowo bardzo często wrażliwe, jak i ogromną ilość podmiotów uprawnionych do gromadzenia i przetwarzania danych medycznych a także jeszcze większą ilość podmiotów uprawnionych do dostępu do tych danych. Podmioty przetwarzające dane medyczne to grupa bardzo różnorodna pod względem prawnym, organizacyjnym a także wielkościowym. Od dużych szpitali poprzez poradnie, przychodnie po indywidualne praktyki, wszystkie one muszą gromadzić i przetwarzać dane medyczne, a także przesyłać i odbierać dane. Dodatkowym czynnikiem wpływającym na bezpieczeństwo danych jest bardzo duża liczba potencjalnych użytkowników systemu, często o różnym przygotowaniu i umiejętnościach pracy z systemami komputerowymi. Także środowisko w którym funkcjonują systemy informacyjne wymaga często bardzo szybkich i niestandardowych operacji dostępu do danych medycznych. Zasygnalizowane powyżej, problemy specyfiki przetwarzania danych medycznych wskazują

7 Współadministrator" Jeśli kilku administratorów wspólnie określa cele i środki przetwarzania danych osobowych, współadministrator danych ustalają zakres odpowiedzialności za zgodność z obowiązkami wynikającymi z niniejszego rozporządzenia spoczywającej na każdym z nich, w szczególności jeśli chodzi o procedury i mechanizmy wykonania praw podmiotu danych, w drodze wspólnych ustaleń. Porozumienie należycie odzwierciedla odpowiednie faktyczne role współadministratora i relacje z podmiotami danych, a istotna treść porozumienia jest udostępniana podmiotowi danych. W przypadku braku jasności co do odpowiedzialności administratorzy ponoszą solidarną odpowiedzialność. Poprawka 119 Wniosek dotyczący rozporządzenia Artykuł 24 Rezolucja ustawodawcza Parlamentu Europejskiego z dnia 12 marca 2014 r. w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (ogólne rozporządzenie o ochronie danych) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)

na trudne wyzwanie jakim będzie wprowadzenie nowych regulacji prawnych dotyczących przetwarzania danych osobowych.

Wdrożenie odpowiednich środków technicznych i organizacyjnych

Przepisy nakładają na administratora danych i podmiot przetwarzający[8] obowiązek wdrożenia odpowiednich środków technicznych i organizacyjnych, by zapewnić poziom bezpieczeństwa stosowny do ryzyka związanego z przetwarzaniem, biorąc pod uwagę wyniki oceny skutków w zakresie ochrony danych, uwzględniając najnowsze osiągnięcia techniczne oraz koszty ich wdrożenia.

Środki techniczne i organizacyjne zapewniające bezpieczeństwo danych to:

a) zapewnienie dostępu do danych wyłącznie przez uprawniony personel w dozwolonych prawem celach,

b) ochrona przechowywanych lub przekazywanych danych osobowych przed ich przypadkowym lub niezgodnym z prawem zniszczeniem, przypadkową utratą lub zmianą oraz nieuprawnionym lub bezprawnym przechowywaniem, przetwarzaniem, dostępem lub ujawnieniem;

c) wprowadzanie w życie polityki bezpieczeństwa w odniesieniu do przetwarzania danych osobowych[9].

Najnowsze osiągnięcia techniczne należy wdrożyć, aby zapewnić:

a) zdolność do poświadczenia integralności danych osobowych;

---

[8] „podmiot przetwarzający" Jeśli przetwarzanie jest realizowane w imieniu administratora, administrator wybiera podmiot przetwarzający dający wystarczające gwarancje wdrożenia odpowiednich środków i procedur technicznych i organizacyjnych, by przetwarzanie odpowiadało wymogom niniejszego rozporządzenia i gwarantowało ochronę praw podmiotów danych, w szczególności jeśli chodzi o techniczne środki bezpieczeństwa i środki organizacyjne regulujące przetwarzanie, które ma być prowadzone, oraz zapewnia zgodność z tym środkami. Poprawka 121 Wniosek dotyczący rozporządzenia Artykuł 26 Rezolucja ustawodawcza Parlamentu Europejskiego z dnia 12 marca 2014 r. w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (ogólne rozporządzenie o ochronie danych) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)

9 Poprawka 124 Wniosek dotyczący rozporządzenia Artykuł 30 Wniosek dotyczący rozporządzenia Artykuł 26 Rezolucja ustawodawcza Parlamentu Europejskiego z dnia 12 marca 2014 r. w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (ogólne rozporządzenie o ochronie danych) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)

b) zdolność do zapewnienia na bieżąco poufności, integralności, dostępności i odporności systemów i usług przetwarzających dane osobowe;

c) zdolność do terminowego przywrócenia dostępności danych i dostępu do nich na wypadek fizycznego lub technicznego incydentu (np. przerwa w dostawie prądu lub Internetu), który oddziałuje na dostępność, integralność i poufność systemów informacji i usług;

d) dodatkowe środki bezpieczeństwa, w przypadku przetwarzania danych osobowych szczególnie wrażliwych aby zapewnić sytuacyjną wiedzę na temat ryzyka i zdolność do podejmowania działań prewencyjnych, naprawczych i łagodzących jego skutki w czasie zbliżonym do rzeczywistego wobec wykrytych słabości oraz incydentów, które mogłyby stanowić zagrożenie dla danych;

e) proces dotyczący regularnego testowania, szacowania i oceniania rozwiązań, procedur i planów bezpieczeństwa przyjętych celem zapewnienia na bieżąco efektywności.

Uwzględniając najnowsze osiągnięcia techniczne, obecny stan wiedzy, najlepsze praktyki w skali międzynarodowej oraz ryzyko, z jakim wiąże się przetwarzanie danych , administrator i ewentualny podmiot przetwarzający , zarówno w momencie ustalania celów i środków niezbędnych do przetwarzania, jak i w momencie samego przetwarzania, wdraża odpowiednie środki i procedury techniczne i organizacyjne, tak by przetwarzanie odpowiadało wymogom rozporządzenia oraz gwarantowało ochronę praw podmiotu danych. Ochrona danych już w fazie projektowania powinna w szczególności uwzględniać cały cykl zarządzania danymi osobowymi od ich zebrania, przez przetwarzanie, do ich usunięcia, systematycznie skupiając się na całościowych gwarancjach proceduralnych odnoszących się do dokładności, poufności, integralności, bezpieczeństwa fizycznego i usunięcia danych osobowych. Jeśli administrator przeprowadził ocenę skutków w zakresie ochrony danych, jej wyniki uwzględnia się przy opracowywaniu wspomnianych środków i procedur. Administrator zapewnia , by domyślnie przetwarzane były jedynie te dane osobowe, które są niezbędne dla realizacji każdorazowego szczególnego celu przetwarzania oraz by w szczególności nie były one zbierane, zatrzymywane lub rozpowszechniane dłużej niż przez okres niezbędny do realizacji tych celów, zarówno jeśli chodzi o ilość danych, jak i okres ich przechowywania. Mechanizmy te zapewniają w szczególności, by dane osobowe nie były domyślnie

udostępniane nieograniczonej liczbie osób oraz by podmioty danych były w stanie kontrolować rozpowszechnianie swoich danych osobowych[10].

Dane Medyczne – szczególne ryzyko – ocena skutków przewidywanych

Jeśli operacje przetwarzania stwarzają szczególne ryzyko dla praw i wolności podmiotów danych z racji swego charakteru, zakresu lub celów, administrator lub podmiot przetwarzający dane, przeprowadzają ocenę skutków przewidywanych operacji przetwarzania w zakresie ochrony danych osobowych.

Szczególne ryzyko jest związane między innymi z operacjami dotyczącymi:

a) systematycznej i kompleksowej oceny aspektów osobowych osoby fizycznej, w tym przetwarzania mające na celu analizę lub przewidzenie w szczególności sytuacji ekonomicznej, miejsca pobytu, stanu zdrowia, preferencji osobistych, wiarygodności lub zachowania osoby fizycznej, która opiera się na automatycznym przetwarzaniu, i na której opierają się środki, które wywołują skutki prawne dotyczące danej osoby lub mają na nią istotny wpływ;(np. do celów ubezpieczeniowych)

b) przetwarzania informacji na temat życia seksualnego, stanu zdrowia, rasy i pochodzenia etnicznego oraz świadczenia usług opieki zdrowotnej, badań epidemiologicznych lub badań mających na celu wykrycie chorób psychicznych bądź zakaźnych, jeśli dane są przetwarzane w celu podjęcia na szeroką skalę środków lub decyzji dotyczących konkretnych osób ;(np. dane o stanie zdrowia przetwarzane przez NFZ)

Ocena skutków przewidywanych operacji przetwarzania obejmuje przynajmniej:

- ocenę ryzyk dla praw i wolności podmiotów danych,
- środki przewidywane w celu sprostania ryzykom, gwarancje, środki i mechanizmy bezpieczeństwa mające zagwarantować ochronę danych osobowych oraz wykazać zgodność z rozporządzeniem, uwzględniając prawa i słuszne interesy podmiotów danych i innych zainteresowanych osób.

10 Poprawka 118 Wniosek dotyczący rozporządzenia Artykuł 23 Rezolucja ustawodawcza Parlamentu Europejskiego z dnia 12 marca 2014 r. w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (ogólne rozporządzenie o ochronie danych) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)

Ocena skutków w zakresie ochrony danych powinna konsekwentnie uwzględniać cały cykl zarządzania danymi osobowymi od ich zebrania, przez przetwarzanie, do ich usunięcia, opisując przy tym szczegółowo planowane operacje przetwarzania, ryzyko dla praw i wolności podmiotów danych, środki przewidywane w celu sprostania ryzyku, gwarancje, środki bezpieczeństwa i mechanizmy mające na celu zapewnienie zgodności z rozporządzeniem.

Oceny skutków są niezbędnym centralnym elementem wszelkich zrównoważonych ram ochrony danych, gdyż dzięki nim przedsiębiorstwa są od samego początku świadome wszelkich możliwych konsekwencji prowadzonych przez nie operacji przetwarzania danych. Jeżeli oceny skutków są starannie przeprowadzane, prawdopodobieństwo operacji naruszającej ochronę danych lub ochronę prywatności może zostać zasadniczo ograniczone[11].

Administratorzy powinni skupić się na ochronie danych osobowych w całym cyklu życia danych – od ich zebrania, przez przetwarzanie, do ich usunięcia – inwestując od samego początku w zrównoważone ramy zarządzania danymi, a następnie wprowadzając kompleksowy mechanizm zgodności[12].

Jeśli ocena skutków w zakresie ochrony danych wykaże, że operacje przetwarzania wiążą się z wysokim poziomem konkretnego ryzyka dla praw i wolności podmiotów danych, takiego jak pozbawienie osób fizycznych przysługującego im prawa, przed rozpoczęciem operacji należy zasięgnąć opinii inspektora ochrony danych lub organu nadzorczego na temat ryzykownego przetwarzania, które mogłoby być niezgodne z przepisami, oraz przedstawić propozycje naprawienia tej sytuacji. Administratorzy danych powinni dokonywać okresowych przeglądów pod kątem zgodności z zasadami ochrony danych w celu wykazania, że stosowane mechanizmy przetwarzania danych są zgodne z wnioskami sformułowanymi w ocenie skutków w zakresie ochrony danych. Przegląd ten powinien również wykazać zdolność administratora danych do respektowania niezależnych

[11] Poprawka 44 Wniosek dotyczący rozporządzenia Motyw 71 a (nowy) Rezolucja ustawodawcza Parlamentu Europejskiego z dnia 12 marca 2014 r. w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (ogólne rozporządzenie o ochronie danych) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)

12 Poprawka 45 Wniosek dotyczący rozporządzenia Motyw 71 b (nowy) Rezolucja ustawodawcza Parlamentu Europejskiego z dnia 12 marca 2014 r. w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (ogólne rozporządzenie o ochronie danych) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)

wyborów dokonanych przez podmioty danych. Ponadto w przypadku, gdy w wyniku przeglądu wykazane zostaną niezgodności, należy je wyszczególnić oraz przedstawić zalecenia dotyczące sposobu osiągnięcia pełnej zgodności[13]

Analiza ryzyka poddawana jest przeglądowi najpóźniej po upływie roku lub natychmiast, jeżeli charakter, zakres lub cele operacji przetwarzania danych ulegną znaczącej zmianie[14].

Po dokonaniu oceny ryzyk administrator i podmiot przetwarzający podejmują środki :

- by chronić dane osobowe przed ich przypadkowym lub niezgodnym z prawem zniszczeniem bądź przypadkową utratą,
- oraz by zapobiec wszelkim innym formom niezgodnego z prawem przetwarzania, w szczególności nieuprawnionemu ujawnieniu, rozpowszechnieniu, dostępowi lub zmianie danych osobowych.

Uwzględniając najnowsze osiągnięcia techniczne oraz koszty wdrożenia, administrator, zarówno w momencie ustalania środków niezbędnych do przetwarzania, jak i w momencie samego przetwarzania, wdraża odpowiednie środki i procedury techniczne i organizacyjne, tak by przetwarzanie odpowiadało wymogom rozporządzenia oraz gwarantowało ochronę praw podmiotu danych.

Administrator obciążany jest zadaniem wdrażania tylko tych środków, które są proporcjonalne do ryzyka przetwarzania danych wynikającego z charakteru danych osobowych, które mają zostać poddane przetwarzaniu.

Ochrona praw i wolności podmiotów danych w zakresie przetwarzania danych osobowych wymaga podjęcia odpowiednich środków technicznych i organizacyjnych, zarówno przy przygotowywaniu przetwarzania, jak i podczas samego przetwarzania.

---

13 Poprawka 48 Wniosek dotyczący rozporządzenia Motyw 74 a (nowy) Rezolucja ustawodawcza Parlamentu Europejskiego z dnia 12 marca 2014 r. w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (ogólne rozporządzenie o ochronie danych) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)

14 Artykuł 32a Rezolucja ustawodawcza Parlamentu Europejskiego z dnia 12 marca 2014 r. w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (ogólne rozporządzenie o ochronie danych) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)

Administrator powinien przyjąć wewnętrzne zasady i wdrożyć odpowiednie środki, które są w szczególności zgodne z zasadą uwzględnienia ochrony danych już w fazie projektowania oraz zasadą domyślnej ochrony danych. Zasada uwzględniania ochrony danych już w fazie projektowania wymaga wbudowania ochrony danych w cały cykl życia technologii, od wczesnego etapu projektowania, aż po ostateczne uruchamianie, stosowanie i ostateczne usuwanie. Powinno to obejmować również odpowiedzialność za produkty i usługi, z których korzysta administrator lub podmiot przetwarzający. Zasada domyślnej ochrony danych wymaga, aby ustawienia dotyczące prywatności w usługach i produktach były domyślnie zgodne z ogólnymi zasadami ochrony danych, takimi jak zasada minimalizacji danych i zasada celowości[15].

Bez wątpienia największym problemem organizacyjnym przed jakim staną kierownicy podmiotów leczniczych będzie rozważenie możliwości lub konieczności (w niedługim czasie) – w przypadku spełniania prawnych kryteriów wynikających z treści rozporządzenia – usytuowania w strukturze organizacyjnej podmiotu leczniczego Administratora Bezpieczeństwa Informacji.

Mimo, że instytucja ta nie jest nowa, funkcjonowała w strukturach wielu instytucji świadczących usług zdrowotne- to od początku 2015 roku została zasadniczo zmieniona.

Administrator Bezpieczeństwa Informacji – inspektor ochrony danych

Prawo nakłada na administratora danych szereg obowiązków związanych z zabezpieczeniem danych oraz obowiązek prowadzenia dokumentacji opisującej sposób przetwarzania danych oraz środki organizacyjne i techniczne podjęte w celu należytej ich ochrony. Muszą one być odpowiednie do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinny zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem[16].

15 Poprawka 37 Wniosek dotyczący rozporządzenia Motyw 61- Rezolucja ustawodawcza Parlamentu Europejskiego z dnia 12 marca 2014 r. w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (ogólne rozporządzenie o ochronie danych)

16 Art. 36. 1. Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych. Dz.U. 1997 nr 133 poz. 883

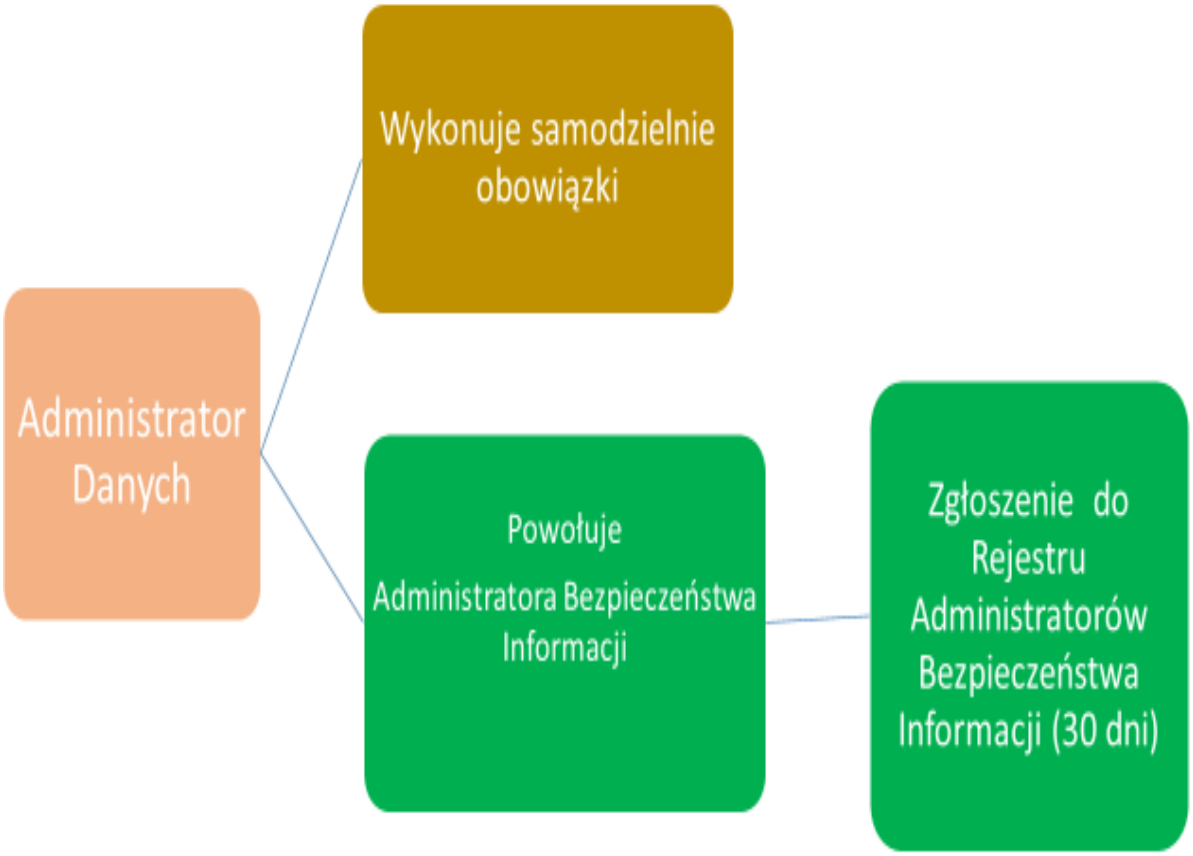
Administrator musi podjąć decyzję, czy powyższe zadania będzie wykonywał sam, czy powoła Administratora Bezpieczeństwa Informacji. Przepis przewiduje wyraźnie dobrowolność ustanowienia instytucji Administratora Bezpieczeństwa Informacji[17]. Alternatywne rozwiązanie to samodzielne sprawowanie wszystkich zadań nałożonych przez przepisy przez administratora danych. W przypadku niepowołania ABI, administrator danych jest zobowiązany samodzielnie wypełnić zadania wskazane powyżej, poza obowiązkiem przygotowywania sprawozdania dla administratora danych osobowych i prowadzenia rejestru zbiorów danych osobowych. (Rysunek 1.)

Inaczej problem powołania ABI regulują przepisy rozporządzenia. W przepisach UE ABI nosi nazwę inspektora ochrony danych.

Administrator i podmiot przetwarzający wyznaczają inspektora ochrony danych, w każdym przypadku, w którym:
a) przetwarzania dokonuje organ lub podmiot publiczny; lub
b) w sektorze prywatnym jeżeli przetwarzanie odnosi się do ponad 5000 podmiotów danych w ciągu 12 miesięcy, niezależnie od wielkość przedsiębiorstwa, lub jeśli główna działalność przedsiębiorstwa to przetwarzanie danych. Określając, czy przetwarzane są dane dotyczące dużej liczby podmiotów danych, nie powinno się uwzględniać danych zarchiwizowanych, które są ograniczone w ten sposób, że nie podlegają normalnemu dostępowi do danych ani operacjom przetwarzania prowadzonym przez administratora oraz nie mogą być już zmieniane
c) operacje przetwarzania dotyczą danych wrażliwych lub operacje przetwarzania , które wymagają regularnego i systematycznego monitorowania, [18]

Rola i zadania ABI w podmiotach leczniczych zostaną szerzej omówione w odrębnym artykule.

17 Art. 36a. 1 Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych. Dz.U. 1997 nr 133 poz. 883
18 Artykuł 35Rozporzadzenia Poprawka 49 Wniosek dotyczący rozporządzenia
Motyw 75 Rezolucja ustawodawcza Parlamentu Europejskiego z dnia 12 marca 2014 r. w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (ogólne rozporządzenie o ochronie danych) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)



Rysunek 1. Alternatywne możliwości wykonywania obowiązków nakładanych na administratorów danych. Opracowanie własne

Naruszenie ochrony danych osobowych

Naruszenie ochrony danych osobowych, w braku odpowiedniej i szybkiej reakcji, może prowadzić do znacznej straty ekonomicznej i szkód społecznych u danej osoby, w tym oszustwa dotyczącego tożsamości. Z tego względu administrator powinien zawiadomić organ nadzorczy o naruszeniu niezwłocznie, przy czym zakłada się, że oznacza to nie później niż po72 godzinach . W stosownym przypadku do zawiadomienia należy dołączyć stosowne wyjaśnienie powodów opóźnienia. Osoby, których dane osobowe mogłyby ucierpieć wskutek takiego naruszenia, powinny być niezwłocznie zawiadamiane, aby umożliwić im podjęcie niezbędnych środków ostrożności.

Podsumowując, proponowane regulacje dotyczące istotnej funkcji administratora danych obciążają administratora całkowitą odpowiedzialnością za przetwarzanie danych osobowych prowadzone przez niego samego lub w jego imieniu. Dotyczy to w szczególności kwestii

takich jak dokumentacja, bezpieczeństwo danych, ocena skutków, inspektor ochrony danych oraz współpraca z instytucją sprawującą nadzór. Administrator powinien zapewnić zgodność operacji przetwarzania danych z wprowadzanym rozporządzeniem. Powinno to być weryfikowane przez niezależnych audytorów wewnętrznych lub zewnętrznych.

Literatura

1. ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (ogólne rozporządzenie o ochronie danych)
2. Rezolucja ustawodawcza Parlamentu Europejskiego z dnia 12 marca 2014 r. w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (ogólne rozporządzenie o ochronie danych) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)
3. Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych. Dz.U. 1997 nr 133 poz. 883
4. DYREKTYWA 95/46/WE PARLAMENTU EUROPEJSKIEGO I RADY z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych
5. STANDARDOWE KLAUZULE UMOWNE, WIĄŻĄCE REGUŁY KORPORACYJNE - JAKIE MAJĄ ZNACZENIE DLA PRZETWARZANIA DANYCH OSOBOWYCH? – portal E-ochronadanych.pl
6. Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych. Dz.U. 1997 nr 133 poz. 883 Strona Unii Europejskiej http://europa.eu/eu-law/decision-making/legal-acts/index_pl.htm
7. Ustawa z dnia 7 listopada 2014 r. o ułatwieniu wykonywania działalności gospodarczej Dz. U. 2014 poz. 1662
8. Komisja Europejska Memo http://europa.eu/rapid/press-release_MEMO-14-186_pl.htm
9. J.Bardadyn Kiedy (ostatecznie!) i jak UE zreformuje prawo ochrony danych osobowych? http://blog-daneosobowe.pl/ue-ostatecznie-zreformuje-prawo-ochronie-danych-osobowych-beda-kluczowe-zalozenia/
10. Ł. Onysyk Jak prowadzić rejestr zbiorów danych osobowych http://blog.e-odo.pl/2015/01/13/jak-prowadzic-rejestr-zbiorow-danych-osobowych/
11. P.Janiszewski Projekt rozporządzenia w sprawie realizacji zadań przez ABI http://blog.e-odo.pl/2015/01/05/projekt-rozporzadzenia-w-sprawie-realizacji-zadan-przez-abi/
12. K.Chylińska Nowe rozporządzenie w sprawie abi http://blog.e-odo.pl/author/katarzyna-chylinska/
13. K.Witkowska Reforma ochrony danych osobowych - nowe obowiązki, nowe korzyści https://www.portalodo.com/entry/reforma-ochrony-danych-osobowych-nowe-obowiazki-nowe-korzysci.
14. P. Wierzbicki Jest szansa na unijne rozporządzenie o ochronie danych (2014.02.11) Obserwator Konstytucyjny http://www.obserwatorkonstytucyjny.pl/debaty/jest-szansa-na-unijne-rozporzadzenie-o-ochronie-danych/

Streszczenie

Od początku 2015 r. weszły w życie nowe przepisy dotyczące ochrony danych osobowych, a prawdopodobnie od 2016 r. na obszarze Unii Europejskiej zostanie wprowadzone rozporządzenie UE regulujące ochronę danych osobowych - projekt Komisji Europejskiej i Parlamentu Europejskiego, które zastąpi Dyrektywę UE 95/46/WE o ochronie danych osobowych. Regulacje te podkreślają fundamentalną rolę administratora danych w zapewnieniu bezpieczeństwa danych osobowych. Administrator danych obciążony jest całkowitą odpowiedzialnością za przetwarzanie danych osobowych prowadzone przez niego samego lub w jego imieniu. Dotyczy to w szczególności kwestii takich jak dokumentacja, bezpieczeństwo danych, ocena skutków, inspektor ochrony danych oraz współpraca z instytucją sprawującą nadzór.